REMARKS

The Examiner is thanked for the performance of a thorough search.

Claims 1, 19, 21, 23, 25, 27, 29, and 31 have been amended. Claims 48-62 have been newly added. No claims have been canceled. Hence, Claims 1, 4-21, 23-25, 27-29, 31-32, 34-37, 39-42, and 44-62 are pending in the present application.

Each issue raised in the Office Action mailed on August 31, 2009 is addressed hereinafter.

I. ISSUES RELATING TO THE CITED ART

A. INDEPENDENT CLAIM 1

Claim 1 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over Bosler, U.S. Patent Application Publication No. US 2005/0010757 ("BOSLER") in view of Kinnis et al., U.S. Patent No. 6,959,382 ("KINNIS"), further in view of Sudia et al., U.S. Patent Application Publication No. US 2002/0013898 ("SUDIA"), and further in view of Mott et al., U.S. Patent No. 6,170,060 ("MOTT"). The rejection is respectfully traversed.

a. BOSLER, KINNIS, SUDIA, and MOTT do not describe the "collective authority" features of Claim 1.

Among other features, Claim 1 comprises the features of:

> ... ;
> verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the one or more configuration directives on the host network element;
> wherein, in accordance with the collective authority, the first user is responsible for the first portion of the one or more configuration directives, the second user is responsible for the second portion of the one or more configuration directives, and the first portion and the second portion of the one or more configuration directives are to be applied to the host network element at the same time;
> ... .

It is respectfully submitted that BOSLER, KINNIS, SUDIA, and MOTT do not describe or suggest the above features of Claim 1. Specifically, BOSLER KINNIS, SUDIA, and MOTT do

not describe or even suggest that two or more users can have **collective authority** to **apply** configuration directives on a network element.

The Office Action asserts that in paragraph [0250] SUDIA describes a concept of collective authority that corresponds to the above features of Claim 1. This assertion is incorrect.

In paragraph [0250], SUDIA describes that when a delegate wants to sign a document on behalf of a primary user, the delegate prepares and signs a request to be communicated to the primary user's smart card. "If multiple delegates need to authorize the primary user's card, they may sequentially sign the request in a similar manner to the way multiple authorizing agents sign a request submitted to a signing device as discussed above." (SUDIA, paragraph [0250].) Apparently, this passage of SUDIA refers to a functionality in which multiple authorizing agents authorize, by sequentially signing a copy of a document, a single signing device to affix the signing device's signature to the document. (See SUDIA, Fig. 12, and paragraphs [0156]-[0165]; specifically, see paragraph [0161].) Thus, the passage from paragraph [0250] of SUDIA, which refers to "multiple delegates", in fact describes how multiple delegates can authorize a primary user's smart card to affix the smart card's signature to a document.

In contrast, the above features of Claim 1 indicate that two or more principals respectively associated with the two or more digital signatures have collective authority to **perform** one or more **configuration directives** on the host **network element**, where, in accordance with the collective authority, a first user is responsible for a first portion of the one or more configuration directives, a second user is responsible for a second portion of the one or more configuration directives, and the first portion and the second portion of the one or more configuration directives are to be applied to the host network element at the same time. However, a functionality of multiple delegates authorizing a single smart card to affix its signature to a document (as described in SUDIA) does not correspond to a functionality of verifying that two

or more users, who are responsible for different portions of configuration directives, have the collective authority to apply the different portions of the configuration directives to a network element at the same time (as featured in Claim 1). Thus, SUDIA does not describe the above features of Claim 1.

Further, BOSLER, KINNIS, MOTT do not cure the above deficiency of SUDIA. Specifically, BOSLER, KINNIS, and MOTT do not describe that two or more users may be responsible for different portions of the same configuration directives, where the two or more users have collective authority to **apply** configuration directives on a network element.

For the foregoing reasons, BOSLER, KINNIS, MOTT, and SUDIA do not describe the above "collective authority" features of Claim 1.

b. BOSLER, KINNIS, SUDIA, and MOTT do not describe the feature of Claim 1 of wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user.

The Office Action asserts that MOTT describes hash generation for a portion of a message and hash generation for a second (or next) portion of the message. Further, the Office Action asserts that this description of MOTT corresponds to the feature of Claim 1 of wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user. This assertion is incorrect.

MOTT describes a method for playing a digital information file on a playback device. Specifically, a device ID and/or a group ID is embedded in the playback device. A device ID or a group ID is also embedded in the digital information file. Upon receiving the digital information file, the device ID or the group ID of the playback device is compared to the device

ID or group ID that are contained in the digital information file. The digital information file is then played if either the device ID or the group ID of the digital information file matches that of the playback device. (See MOTT, col. 2, lines 9-19.)

Significantly, however, MOTT expressly describes that: (1) the hashes are computed automatically **from** each "n" seconds of the program data stored in the digital information file (see MOTT, col. 18, lines 62-64 and col. 19, lines 26-29); and (2) the computed hashes are used to ensure that the digital information file has not been altered (see MOTT, col. 18, 55-59.)

In contrast, Claim 1 includes the feature of wherein the two or more digital signatures comprise a first digital signature of **a first portion** of the one or more configuration directives by a first user, and a second digital signature of a **second portion** of the one or more configuration directives by a second user. Since the hashes in MOTT are computed from portions of a digital information file automatically and are not associated with any users, MOTT does not describe the above features of Claim 1. Further, the functionality of using the computed hashes to ensure that the digital information file has not been altered (as described in MOTT) does not correspond to the functionality of using two or more digital signatures, by two or more users on two or more different portions of the same configuration directives, to verify that the two or more users have collective authority to perform the one or more configuration directives on a network element at the same time (as featured in Claim 1).

Further, BOSLER, KINNIS, and SUDIA do not cure the above deficiency of MOTT. Specifically, BOSLER, KINNIS, and SUDIA do not describe that different portions of the same **configuration directives** can be signed with different signatures by two or more different users.

For the foregoing reasons, BOSLER, KINNIS, MOTT, and SUDIA do not describe the above features of Claim 1.

c. BOSLER, KINNIS, SUDIA, and MOTT do not describe the features of Claim 1 of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.

The Office Action asserts that the above features of Claim 1 are described in paragraphs [0058] and [0069] of BOSLER and in col. 8, lines 50-56 of KINNIS. This assertion is incorrect for at least two reasons.

First, it is noted that paragraphs [0058] and [0069] of BOSLER refer to two completely different and separate embodiments – the embodiment in paragraph [0058] refers to establishing secure sessions between nodes by exchanging a management message, while the embodiment in paragraph [0069] refers to a management server that sends management requests to nodes that are being managed. In other words, paragraph [0058] of BOSSLER describes that two nodes can establish a secure session, while paragraph [0069] describes that a central management server can send requests to agents on the nodes for information about the function of the agents' respective nodes. Significantly, neither paragraphs [0058] and [0069] nor any other passage of BOSLER describes a management message that includes a number of required signatures and required principals. Further, BOSSLER does not describe a functionality of determining whether to apply a configuration command by checking or otherwise determining anything about a number of required signatures and required principals that are associated with a management message.

Second, in col. 8, lines 48-56 KINNIS describes that a digital signature service generates a signature file that contains: a document, a digital signature of a user that signed the document, a certificate, and optionally additional file attributes. The additional file attributes may include

an attribute (i.e., multiple signature attribute) that indicates the number of times the file has been signed. Significantly, KINNIS does not describe or suggest any functionality of using the multiple signature attribute to determine whether to apply a configuration command on a network element. Rather, in col. 8, lines 57-61, KINNIS describes that the digital signature service uses the multiple signature attribute to display the appropriate certificates to the user and to extract the original document from the signature file.

In contrast, Claim 1 comprises the features of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. Since BOSLER does not describe a functionality of checking or otherwise determining anything about a number of required signatures and required principals in a management message, and since KINNIs does not describe a functionality of using the multiple signature attribute to determine whether to apply a configuration command on a network element, BOSLER and KINNIS whether taken alone or in combination do not describe the above features of Claim 1.

For the foregoing reasons, BOSLER, KINNIS, SUDIA, and MOTT do not describe or suggest all features of Claim 1. Thus, Claim 1 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS, further in view of SUDIA, and further in view of MOTT. Reconsideration and withdrawal of the rejection of Claim 1 is respectfully requested.

B. INDEPENDENT CLAIM 8

Claim 8 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS, and further in view of SUDIA. The rejection is respectfully traversed.

Among other features, Claim 8 comprises the features of:

receiving **configuration control information** that **includes a time period during which a valid digital signature is required for applying one or more particular configuration directives**;

...;

determining if the one or more configuration directives have been previously received during the time period;

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, **and applying the configuration directives** to a network element only when the one or more digital signatures are verified successfully;

... .

The Office Action asserts that the above features of Claim 8 are described in paragraphs [0069], [0071], and [0073] of BOSLER and in paragraph [0249] of SUDIA. These assertions are incorrect.

It is respectfully submitted that the time limit for a certificate (as described in paragraph [0249] of SUDIA) does not correspond to the time period featured in Claim 8. In SUDIA, the time limit is tied to a particular certificate and is used to determine whether that particular certificate is valid. If the particular certificate is valid, then a delegate user can use a card that stores that particular certificate. (See SUDIA, paragraph [0250].) In contrast, Claim 8 features a time period during which a check must be made to determine whether the same configuration directives have already been received. Thus, the differences between the functionality of the time limit for the certificate of SUDIA and the functionality of the time period of Claim 8 are significant.

For example, in SUDIA as long as the time limit of a particular certificate has not expired, a delegate user can use a card with that particular certificate to sign any number of document as many times as necessary. (See, for example, SUDIA, paragraphs [0248] and [0250].) In contrast, the above features of Claim 8 indicate that the same configuration directives will be applied only once during the time period specified in a configuration control information that is received at a host network element.

Further, the time interval described in paragraph [0071] of BOSLER is an interval within which a node must request a public key certificate. Significantly, a certificate server would grant a public key certificate to a node only if the node requests the certificate within a particular time interval after a management agent is initialized/installed on the node. (See also at least BOSLER, paragraph [0010]; paragraph [0073], lines 17-22.) Thus, the time interval described in paragraph [0071] of BOSLER is used to determine whether or not a node would be granted a public key certificate, which is very different from a functionality of determining whether the same configuration directives have been previously received at a host network element within a specified time period, as featured in Claim 8.

Finally, it is noted that Claim 8 includes the feature of **determining if the one or more configuration directives have been previously received during the time period**. The Office Action asserts that in paragraph [0069] BOSLER describes a functionality of processing configuration commands within a time period. This assertion is factually incorrect. In paragraph [0069], BOSLER describes that a central management server can send requests to agents on the nodes for information about the function of the agents' respective nodes. Significantly, however, in paragraph [0069] BOSLER does not describe anything about a time period. Further, as discussed above, the time limit described in SUDIA is tied to a particular certificate and is used to determine whether the certificate is valid. Thus, BOSLER and SUDIA do not describe or even suggest the functionality featured in Claim 8 of determining if the same configuration directives have been previously received at a network element during a specified time period.

For the above reasons, BOSLER, KINNIS, and SUDIA do not describe or suggest all features of Claim 8. Thus, Claim 8 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of SUDIA. Reconsideration and withdrawal of the rejection of Claim 8 is respectfully requested.

C. INDEPENDENT CLAIM 18

Claim 18 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS and further in view of SUDIA.

Claim 18 includes features similar to the features of Claim 8 discussed above. Thus, Claim 18 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS and further in view of SUDIA for at least the reasons given above with respect to Claim 8. Reconsideration and withdrawal of the rejection of Claim 18 is respectfully requested.

D. INDEPENDENT CLAIMS 21, 25, AND 29

Claims 21, 25, and 29 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS, further in view of SUDIA, and further in view of MOTT.

Claims 21, 25, and 29 include features similar to the features of Claim 1 discussed above, except in the context of an apparatus and a computer-readable medium. Thus, Claims 21, 25, and 29 are patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS, further in view of SUDIA, and further in view of MOTT for at least the reasons given above with respect to Claim 1. Reconsideration and withdrawal of the rejection of Claims 21, 25, and 29 is respectfully requested.

E. DEPENDENT CLAIMS 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, AND 44-47

Claims 4-7, 20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS, further in view of SUDIA, and further in view of MOTT. Claims 9-17 and 19 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS and further in view of SUDIA.

Each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 depends

from one of independent Claims 1, 8, 18, 21, 25, and 29, and thus includes each and every feature of the independent base claim. Thus, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is allowable for at least the reasons given above for Claims 1, 8, 18, 21, 25, and 29. In addition, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those features is not included at this time. Therefore, it is respectfully submitted that Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 are allowable for the reasons given above with respect to Claims 1, 8, 18, 21, 25, and 29. Reconsideration and withdrawal of the rejections of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is respectfully requested.

F. NEW CLAIMS 48-62

New independent Claim 48 includes features similar to the features of Claim 8 discussed above, except in the context of a computer-readable volatile or non-volatile medium. New independent Claim 60 includes features similar to the features of Claim 18 discussed above, except in the context of a computer-readable volatile or non-volatile medium. Thus, Claims 48 and 60 are allowable for at least the reasons given above with respect to Claims 8 and 18, respectively. Consideration and allowance of Claims 48 and 60 is respectfully requested.

Each of new dependent Claims 49-59 and 61-62 depends directly or indirectly from one of new independent Claims 48 and 60, and thus includes each and every feature of the corresponding base claim. Thus, each of Claims 49-59 and 61-62 is allowable for at least the reasons given above for Claims 48 and 62. In addition, each of Claims 49-59 and 61-62 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a

separate discussion of those features is not included at this time. Therefore, it is respectfully submitted that Claims 49-59 and 61-62 are allowable for the reasons given above with respect to Claims 48 and 62. Consideration and allowance of Claims 49-59 and 61-62 is respectfully requested.

II. CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed. Further, for the reasons set forth above, the Applicant respectfully submits that allowance of the pending claims is appropriate. Reconsideration of the present application is respectfully requested in light of the amendments and remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: November 30, 2009

/StoychoDDraganoff#56181/
Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076